



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,804	02/12/2002	Denis Jacques Paul Garcia	PA2904US	7096
22830	7590	06/28/2006	EXAMINER	
CARR & FERRELL LLP 2200 GENG ROAD PALO ALTO, CA 94303				CHAI, LONGBIT
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 06/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/074,804	GARCIA, DENIS JACQUES PAUL	
	Examiner Longbit Chai	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 22 June 2002.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-38 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 2/12/2002 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

## **DETAILED ACTION**

1. Original application contained claims 1 – 38. Claims 1 – 35 have been amended in an amendment filed on 6/22/2006. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 38.

### ***Continued Examination Under 37 CFR 1.114***

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/22/2006 has been entered.

### ***Response to Arguments***

3. As per claim 1 and 33, Applicant asserts that Ginter does not contemplate "a client module configured to generate a header comprising encrypted security information as to who and how a file including the electronic data can be accessed" (Page 4, 2<sup>nd</sup> Para). Examiner notes Applicant's arguments have been fully considered but are not persuasive with the following reasons: (a) a data message is considered to have two separate portions, namely, header portion and content portion. In view of Figure 17, as taught by Ginter, the data message comprises the content portion having

elements, for example, Element 812a – 812c, etc. and header portion, having public header, private header, private body (Method 1000) and permission records (including key block(s)) as shown, for example, Element 802 – 810, (b) Ginter teaches one of the header portion, the "permission record" (Element 808), specifies the rights associated with the object such as who can use the object's content as well as user's rights to use its content (Ginter: Column 59 Line 6 – 18) and another one of the header portion, the "Method 1000" (Element 806), defines how the object content can be used by the user (i.e. access rule) such as allowing unlimited viewing within a fixed period of time for a fixed fee (Ginter: Column 128 Line 31 – 36), and (c) Ginter also teaches "permission records 808" and key blocks (810) can be encrypted with a private DES key (Ginter: Column 129 Line 18 – 20) as well as the "Method 1000 (i.e. private body)" is preferably encrypted using one or more private body keys contained in the separate permission records (Ginter: Column 130 Line 35 – 37). Therefore, Ginter does teach "a client module configured to generate a header comprising encrypted security information as to who and how a file including the electronic data can be accessed" and as such applicant's arguments are respectfully traversed.

4. As per claim 17, Applicant asserts that Ginter does not teach "header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data" (Page 5, Last Para). Examiner notes Applicant's arguments have been fully considered but are not persuasive with the similar rationale as set forth above because Ginter also teaches the private body (Method 1000),

defining access rules, having N encrypted segments can be encrypted using one or more private body keys contained in the separate permission records 808 (Ginter: Column 130 Line 35 – 37 and Column 128 Line 31 – 36). Therefore, Ginter does teach "header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data" and as such applicant's arguments are respectfully traversed.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 – 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter (Patent Number: 6253193).

As per claim 1 and 33, Ginter teaches a system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, comprising:

a client module configured to generate a header comprising encrypted security information as to who and how a file including the electronic data can be accessed, and (Ginter: Figure 17 & Column 59 Line 6 – 18, Column 128 Line 31 – 36, Column 129 Line 18 – 20 and Column 130 Line 35 – 37: one of the header portion, the “permission record” (Element 808), specifies the rights associated with the object such as who can use the object’s content as well as user’s rights to use its content (Column 59 Line 6 – 18) and another one of the header portion, the “Method 1000” (Element 806), defines how the object content can be used by the user (i.e. access rule) such as allowing unlimited viewing within a fixed period of time for a fixed fee (Column 128 Line 31 – 36), and (c) Ginter also teaches “permission records 808” and key blocks (810) can be encrypted with a private DES key (Column 129 Line 18 – 20) as well as the “Method 1000 (i.e. private body)” is preferably encrypted using one or more private body keys contained in the separate permission records (Column 130 Line 35 – 37));

Configure to generate an encrypted data portion comprising the file encrypted with a file key according to a predetermined cipher scheme (Ginter: Column 128 Line 41 – 65),

wherein the header is coupled to the encrypted data portion to generate a secured file (Ginter: Figure 17 & 18).

As per claim 17, Ginter teaches a system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, the format comprising:

a client module configured to generate a header including a file key encrypted and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data, wherein N >= 1 (Ginter: Figure 17 &18, Column 129 Line 18 – 20. Column 128 Line 45 – 65 and Column 59 Line 6 – 18, Column 128 Line 31 – 36, Column 129 Line 18 – 20 and Column 130 Line 35 – 37: the private body (Method 1000), defining access rules, having N encrypted segments can be encrypted using one or more private body keys contained in the separate permission records 808 (Column 130 Line 35 – 37 and Column 128 Line 31 – 36));

an encrypted data portion including the electronic data encrypted according to a predetermined cipher (Ginter: Column 128 Line 41 – 65);

wherein the header is coupled to the encrypted data portion to generate a secured file, and the file key can be retrieved to decrypt the encrypted data portion only when the access values in one of the N encrypted segments are measured successfully against access privilege associated with a user accessing the, secured file (Ginter: Figure 18 and Column 128 Line 45 – 65).

As per claim 2, Ginter teaches the security information in the header of the secured file facilitates the restricted access to the file (Ginter: Column 128 Line 25 – 40).

As per claim 3 and 35, Ginter teaches the security information is encrypted with a user key associated with a user (Ginter: Column 14 Line 40 – 43).

As per claim 4 and 36, Ginter teaches the user is a member selected from a group consisting of a human user, a software agent, a device and a group of users; and wherein the user is granted access privilege to access the file (Ginter: Column 123 Line 38 – 41).

As per claim 5, Ginter teaches the security information includes the file key and access rules to the restricted access to the file (Ginter: Column 130 Line 35 – 40, Column 128 Line 25 – 40 and Figure 17 & 18).

As per claim 6, Ginter teaches the file key is retrieved to decrypt the encrypted data portion in the secured file when the access privilege of the user is within access permissions by the access rules (Ginter: Column 128 Line 25 – 65).

As per claim 7 and 26, Ginter teaches the access rules are expressed in a markup language (Ginter: Column 141 Line 36: SGML).

As per claim 8 and 27, Ginter teaches the markup language is Extensible Access Control Markup Language (Ginter: Column 141 Line 36: SGML).

As per claim 9 and 28, Ginter teaches the markup language is selected from a group consisting of HTML, XML and SGML (Ginter: Column 141 Line 36).

As per claim 10, Ginter teaches the secured file is configured to have a file extension identical to what the file originally has so that an application designated to access the file can be executed to access the secured file (Ginter: Figure 17 and Column 14 Line 21 – 28).

As per claim 11, Ginter teaches the security information includes a flag to the application that the secured file being accessed can not be accessed as it normally does (Ginter: Column 137 Line 63 – 66).

As per claim 12, Ginter teaches the flag is configured to be placed in a position of the secured file so that the flag will be accessed first when the secured file is accessed by the application (Ginter: Column 137 Line 63 – 66).

As per claim 13, Ginter teaches the security information includes the file key and access rules, the access rules controlling who and how the secured file can be accessed, and wherein the security information in the header is organized in such a way that the application is paused, upon detecting that the secured file is being accessed, for an access control module to determine whether a user requesting the secured file

has proper access privilege to do so with respect to thE; access rules in the security information (Ginter: Column 128 Line 25 – 40).

As per claim 14, Ginter teaches the access control module operating in a path through which the secured file is confined to be loaded into the application (Ginter: Column 23 Line 56 and Column 23 Line 67).

As per claim 15, Ginter teaches the file key is a symmetric cipher key (Ginter: Column 200 Line 28).

As per claim 16, Ginter teaches the file is one or more of a document, a multimedia file, a set of dynamic or static data, a sequence of executable code, an image and a text (Ginter: Column 14 Line 5 – 28).

As per claim 18, 22 and 34, Ginter teaches the header further includes a user block having user information identifying who can access the secured file (Ginter: Column 128 Line 31).

As per claim 19, Ginter teaches the header further includes each of the N encrypted segments of the rule block includes policies how the secured can be accessed (Ginter: Column 23 Line 44 – 45 and Figure 18 Element 812a – 812n).

As per claim 20, Ginter teaches the user block includes N encrypted segments, each including the file key (Ginter: Column 128 Line 45 – 65).

As per claim 21, Ginter teaches each of the N encrypted segments of the user block corresponds to one of the N encrypted segments of the rule block (Ginter: Column 128 Line 45 – 65).

As per claim 23, Ginter teaches each of the N encrypted segments of the user block further includes cipher information about the predetermined cipher to facilitate a decryption process of the encrypted data portion with the file key (Ginter: Column 128 Line 25 – 65 and Figure 18).

As per claim 24, Ginter teaches the access rules in each of the N encrypted segments of the rule block determine at least an action with which the secured document can be accessed by a user associated with one of the N encrypted segments of the user block (Ginter: Column 128 Line 45 – 65 and Figure 18).

As per claim 25, Ginter teaches the action includes one or more of commands: open, export, read, edit, play, listen to, print or forward and attach (Ginter: Column 128 Line 45 – 65).

As per claim 29, Ginter teaches the N encrypted segments of the user block are respectively encrypted with tine file key (Ginter: Column 128 Line 45 – 65).

As per claim 30, Ginter teaches an authorized user associated with one of the encrypted segments of the user block can view the access rules of each of the N encrypted segments of the rule block when access privilege of the authorized user is measured successfully with the access rules in one of the N encrypted segments in the rule block associated with the authorized user (Ginter: Column 128 Line 30 – 36 and Figure 18).

As per claim 31, Ginter teaches the authorized user can update the access rules of each of the N encrypted segments of the rule block (Ginter: Column 29 Line 44 – 47, Column 32 Line 30 – 39 and Figure 18).

As per claim 32, Ginter teaches the N encrypted segments of the user block remain encrypted every time the secured file is stored in a storage space (Ginter: Column 222 Line 23 – 26).

As per claim 37, Ginter teaches obtaining the access rules from either a default setting for a file place in which the secured file is to be placed or a manual setting in accordance with access privilege associated with a user who is creating the secured file (Ginter: Column 128 Line 25 – 40).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter (Patent Number: 6253193), in view of Folmsbee (Patent Number: 6308256).

As per claim 38, Ginter teaches if the secured file is newly generated, generating the file key from the predetermined cipher (Ginter: Column 206 Line 16 – 21);

However, Ginter does not teach if the secured file is being stored in a storage place, retrieving the file key from a memory store; and deleting the file key from a memory store as soon as the secured file is stored in the storage place.

Folmsbee teaches if the secured file is being stored in a storage place, retrieving the file key from a memory store; and deleting the file key from a memory store as soon as the secured file is stored in the storage place (Folmsbee: Column 16 Line 4: key expiry event as taught by Folmsbee could be real-time (i.e. immediately after use) or number of uses – e.g. Examiner is interpreting the number of uses to be one which would meet the Applicant's claimed language).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Folmsbee within the system of Ginter because Folmsbee teaches providing secure transfer of electronic content through open channel such as internet by using a secure key in configuring the encrypted software (Folmsbee: Column 3 Line 18 – 32 and Column 3 Line 41 – 43).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai  
Examiner  
Art Unit 2131

LBC 

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100